HIPAA BUSINESS PARTNER CHAIN OF TRUST ADDENDUM

THIS ADDENDUM supplements and is made a part of a [identify agreement by name and date] (herein "Agreement") by and between [name hospital]("Hospital") and [name vendor] ("Vendor").

BACKGROUND STATEMENTS

A. Hospital and Vendor are parties to an agreement pursuant to which Vendor provides certain services to Hospital and, in connection with those services, Hospital discloses to Vendor certain information ("Protected Health Information" as further defined below) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191; and

B. Vendor, as a recipient of protected information from Hospital, is a "Business Partner" as that term is defined in HIPAA and regulations promulgated by the U.S. Department of Health and Human Services to implement certain provisions of HIPAA (herein "HIPAA Regulations"); and

C. Pursuant to the HIPAA Regulations, all Business Partners of entities such as Hospital must, as a condition of doing business with Hospital, agree in writing to certain mandatory provisions regarding, among other things, the use and disclosure of Protected Information; and

D. The purpose of this addendum is to satisfy the requirements of the HIPAA Regulations, including, but not limited to, 45 CFR § *164.506(e),* as the same may be amended from time to time.

IN CONSIDERATION OF THE FOREGOING, and of the desire of each party to continue providing or receiving services under the Agreement, the parties agree as follows:

1. **Definitions.**

Unless otherwise provided in this addendum, capitalized terms have the same meaning as set forth in the HIPAA Regulations, 45 CFR parts 142 and 160-164.

2. **Scope of Use of Protected Health Information.** Vendor may not:

a. use or otherwise disclose Protected Health Information (as defined in *45* CFR §164.504) it receives from Hospital for any purpose other than the purpose expressly stated in the Agreement;

b. notwithstanding any other provisions of the Agreement, use or disclose Protected Health Information in the manner that violates or would violate the HIPAA regulations if such activity were engaged in by Hospital.

3. **Safeguards for the Protection of Protected Health Information.**

a. Vendor shall implement and maintain, and by this Addendum warrants that it has implemented, such safeguards as are necessary to ensure that the Protected Health Information disclosed by Hospital to Vendor is not used or disclosed by Vendor except as is provided in the Agreement.

b. Attached hereto as Exhibit A and incorporated herein by reference is a Vendor Security Assessment of the safeguards implemented and maintained by Vendor to prevent unauthorized use or disclosure

of Protected Health Information. Vendor warrants and represents that the information on Exhibit A is true, correct and accurate and that Exhibit A has been completed on behalf of Vendor by one or more persons knowledgeable about Vendor's security systems and procedures. Vendor acknowledges that Hospital is relying on the Vendor Security Assessment in selecting Vendor as a Business Partner. Vendor shall promptly notify Hospital of any material change to any aspect of its security safeguards. Notwithstanding any other provisions of this Agreement to the contrary, Hospital may terminate the Agreement without penalty if it determines, in its sole discretion, that any such changes or any diminution of Vendor's reported security procedures render any or all of Vendor's safeguards unsatisfactory to Hospital. Vendor shall confirm in writing to Hospital, from time to time upon Hospital's request, the continued accuracy of Exhibit A.

4. **Reporting of Unauthorized Use or Disclosure.** Vendor shall promptly report to Hospital any use or disclosure of Protected Health Information of which Vendor becomes aware that is not provided for or permitted in the Agreement. Vendor shall permit Hospital to investigate any such report and to examine Vendor's premises, records and practices.

5. **Use of Subcontractors**. To the extent that Vendor uses one or more subcontractors or agents to provide services under the Agreement, and such subcontractors or agents receive or have access to the Protected Health Information, each such subcontractor or agent shall sign an agreement with Vendor containing substantially the same provisions as this Addendum and further identifying Hospital as a third party beneficiary with rights of enforcement and indemnification from such subcontractors or agents in the event of any violations.

6. **Uses of Open Communication Channels; Encryption**

a. Vendor may not transmit Protected Health Information over the Internet or any other insecure or open communication channel unless such information is encrypted or otherwise safeguarded using procedures no less stringent than those described in *45* CFR § 142.308(d).

b. If Vendor stores or maintains Protected Health Information in encrypted form, Vendor shall, promptly at Hospital's request, provide Hospital with the key or keys to decrypt such information.

7. **Authorized Alteration of Protected Health Information.**

a. Vendor acknowledges that the HIPAA regulations require Hospital to provide access to Protected Health Information to the subject of that information, if and when Vendor makes any material alteration to such information. For purposes of this section, "Material Alteration" means any addition, deletion or change to the Protected Health Information of any subject other than the addition of indexing, coding or other administrative identifiers for the purpose of facilitating the identification or processing of such information.

b. Vendor shall provide Hospital with notice of each material alteration in any Protected Health Information and shall cooperate promptly with Hospital in responding to any request made by any subject of such information to Hospital to inspect and/or copy such information.

c. Vendor may not deny Hospital access to any such information if, in Hospital's sole discretion, such information must be made available to the subject seeking access to it.

d. Vendor shall promptly incorporate all amendments or corrections to protected health information when notified by Hospital that such information is inaccurate or incomplete.

8. **Audits**, **Inspection and Enforcement.**

a. From time to time upon reasonable notice, Hospital may inspect the facilities, systems, books and records of Vendor to monitor compliance with this Addendum. Vendor shall promptly remedy any violation of any term of this Addendum and shall certify the same to Hospital in writing. The fact the Hospital inspects, or fails to inspect, or has the right to inspect, Vendor's facilities, systems and procedures does not relieve Vendor of its responsibility to comply with this Addendum, nor does Hospital's failure to detect, or to detect but fail to call Vendor's attention to or require Remediation of any unsatisfactory practice constitute acceptance of such practice or a waiver of Hospital's enforcement rights.

b. Vendor further agrees to make its internal practices, books and records relating to the use and disclosure of protected health information available to DHHS or its agents for the purposes of enforcing the provisions of this Addendum and the HIPAA regulations.

c. Hospital may terminate the Agreement without penalty if Vendor repeatedly violates this Addendum or any provision hereof, irrespective of whether, or how promptly, Vendor may remedy such violation after being notified of the same. In case of any such termination, Hospital shall not be liable for the payment of any services performed by Vendor after the effective date of the termination, and Hospital shall be liable to Vendor in accordance with the Agreement for services provided prior to the effective date of termination.

d. Vendor acknowledges and agrees that any individual who is the subject of Protected Health Information disclosed by Hospital to Vendor is a third party beneficiary of this Addendum and may, to the extent otherwise permitted by law, enforce directly against Vendor any rights such individual may have under this Addendum, the Agreement, or any other law, relating to or arising out of Vendor's violation of any provision of this Addendum.

9. **Effect of Termination.** Upon the termination of the Agreement for any reason, Vendor will return to Hospital, or, at Hospital's direction, destroy, all Protected Health Information received from Hospital that Vendor maintains in any form, recorded on any medium, or stored in any storage system. A senior officer of Vendor shall certify in writing to Hospital, within five days after the termination or other expiration of the Agreement, that all Protected Health Information has returned or disposed of as provided above and that Vendor no longer retains any such Protected Health Information in any form. Vendor shall remain bound by the provisions of this Addendum, even after termination of the Agreement, until such time as all protected health information has been returned or otherwise destroyed as provided in this section.

10. **Indemnification**. Vendor shall indemnify and hold Hospital harmless from and against all claims, abilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this addendum by Vendor.

11. Disclaimer. HOSPITAL MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY VENDOR WITH THIS ADDENDUM OR THE HIPAA REGULATIONS WILL BE ADEQUATE OR SATISFACTORY FOR VENDOR'S OWN PURPOSES OR THAT ANY INFORMATION IN VENDOR'S POSSESSION OR CONTROL, OR TRANSMITTED OR RECEIVED BY VENDOR, IS

OR WILL BE SECURE FROM UNAUTHORIZED USE OR DISCLOSURE, NOR SHALL HOSPITAL BE LIABLE TO VENDOR FOR ANY CLAIM, LOSS OR DAMAGE RELATED TO THE UNAUTHORIZED USE OR DISCLOSURE OF ANY INFORMATION RECEIVED BY VENDOR FROM HOSPITAL OR FROM ANY OTHER SOURCE. VENDOR IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY VENDOR REGARDING THE SAFEGUARDING OF PROTECTED HEALTH INFORMATION.

12. **Certification.** Subject to compliance with Vendor's security requirements, Hospital, or its authorized agents or contractors, may at Hospital's cost examine Vendor's facilities, systems, procedures and records as may be required by such agents or contractors to certify to Hospital that Vendor's security safeguards comply (or do not comply, as the case may be) with HIPAA, the HIPAA regulations, or this Addendum.

13. **Effect on Agreement.** Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the Agreement shall remain in force and effect.

14. **Construction.** This Addendum shall be construed as broadly as necessary to implement and comply with HIPAA and the HIPAA Regulations. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.

HOSPITAL

_____

_____
Date

VENDOR

_____

_____
Date

EXHIBIT A

VENDOR SECURITY ASSESSMENT
FOR [HOSPITAL NAME]

Name of Vendor:

Services to be provided by Vendor: _____

Date:_____

Vendor: To permit Hospital to assess the measures you currently have in place to safeguard Protected Health Information (as that term is defined in *45* CFR § 164.504) that may be disclosed to you by Hospital, please complete the following survey.

PART 1
GENERAL QUESTIONS

1. How many employees do you have? _____

2. Do you use subcontractors to assist you in performing your contracts? Yes ☐ No ☐

3. Please identify the location of all facilities where you process Protected Health Information.

PART 2
ADMINISTRATIVE PROCEDURES

1. Do you have written agreements with every subcontractor who processes Protected Health Information for you by which the subcontractors agree to protect the integrity and confidentiality of the data exchanged between you?
   Yes ☐ No ☐

2. Do you have a contingency plan in place that provides for the following:

   (a) A written assessment of the sensitivity, vulnerabilities and security of your programs and the information you receive, manipulate, store and transmit?
   Yes ☐ No ☐
   (b) Data backup plan?
   Yes ☐ No ☐
   (c) Disaster recovery plan?
   Yes ☐ No ☐

   (d) Emergency mode operation plan? Yes ☐ No ☐

   (e) Testing and revision procedures to periodically test and revise the contingency plan? Yes ☐ No ☐

3. Do you have written policies documenting your internal procedures for routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of Protected Health Information?
   Yes ☐ No ☐
4. Do you have written policies and procedures establishing the following:

   (a) Rules for granting access to Protected Health Information? Yes☐ No☐

   (b) Rules to determine a person's or entities' initial right of access to a terminal, transaction, program, process or data?
   Yes☐ No ☐
   (c) Rules governing modification of any person's or entities' right of access to a terminal, transaction, program, process or data?
   Yes ☐ No ☐

5. Do you have a regular process of in-house review and audit of the reports and logs of system access activity?
   Yes☐ No☐

6. Do you have written policies and procedures addressing the following personnel security clearance issues:

   (a) Supervision of maintenance personnel by authorized and knowledgeable supervisory personnel?
   Yes ☐ No ☐

   (b) Maintenance of comprehensive and current records of all access authorizations? Yes☐ No☐

   (c) Assuring that operating and maintenance personnel have proper access authorization for their level of responsibility?
   Yes☐ No ☐

   (d) Determining the appropriateness of any individual's access to Protected Health Information?
   Yes☐ No☐

   (e) Requiring all personnel security policies and procedures to be in writing and reviewed periodically?
   Yes☐ No☐

   (f) Requiring all system users, including maintenance personnel, to receive security awareness training regarding the use of Protected Health Information?
   Yes☐ No☐

7. Do you have the following in place to ensure a coherent, comprehensive and integrated enterprise-wide system of security:

   (a) Written security plans, rules, procedures and instructions concerning all components of your security systems?
   Yes☐ No☐

(b) Written policies and procedures for testing and verifying the security attributes of all new hardware and software, as well as periodic testing of the security attributes of existing hardware and software?
Yes☐ No☐

(c) A formal and current inventory of all of your hardware and software assets?
Yes☐ No ☐

(d) A formal process involving hands-on functional testing, penetration testing and verification processes to determine that the security features of your systems are implemented as designed and are adequate for their environment?
Yes☐ No ☐

(e) Virus checking capabilities that identify and disable viruses? Yes☐ No☐

8. Written policies and procedures for reporting breaches of security that includes the following:

(a) Documentation of reported security incidents? Yes☐ No ☐

(b) Responsive actions to be taken when a security incident report has been received? Yes☐ No ☐

9. Do you have in place the following internal controls to ensure the prevention, detection, containment and correction of security breaches:

(a) A process for selection of security/control measures by balancing the costs of security control measures against losses to be expected if such measures were not implemented?
Yes☐ No ☐

(b) Processes for assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that risk level?
Yes ☐ No ☐

(c) Written policies and procedures that are communicated to all employees, agents and contractors identifying the consequences of non-compliance with your security policies and procedures?
Yes☐ No ☐

(d) A written security policy containing a general statement of the importance of the information you process and your responsibility and commitment to protecting that information?
Yes ☐ No ☐

10. Do you have documented procedures related to the termination of an employee's employment or change in status that include the following:

(a) Changing combinations of locking mechanisms, both on a recurring basis and when personnel no longer have a need to know or require access to the protected system? Yes☐ No ☐

(b) Removing or canceling a person's or entities' access privileges immediately when the person or entity no longer requires access to the protected system?
Yes☐ No ☐

(c) Assuring that all keys, key entry cards, or tokens that allow a terminated employee access to your property, buildings, systems or equipment are retrieved and secured prior to termination?
Yes ☐ No ☐

11. Do you have a training program that includes the following:

(a) Awareness training for all personnel that includes, but is not limited to, correct procedures for password maintenance, incident reporting, and awareness in reporting of viruses or other perceived threats to security?

Yes☐ No☐

(b) Periodic refresher training of your employees, agents and contractors concerning your security concerns and responsibilities?

Yes☐ No ☐

(c) Increasing user awareness of the potential harm that can be caused by viruses, how to prevent the introduction of viruses into your systems and appropriate responses if viruses are detected?

Yes ☐ No ☐

(d) User education on reporting log-in discrepancies or incidents? Yes☐ No ☐

(e) User education in password management including rules for creating, changing, storing and preserving the confidentiality of passwords?
Yes☐ No☐

PART 3
PHYSICAL SAFEGUARDS

1. Do you have written policies and procedures to manage and supervise the use of security measures and the conduct of personnel as it relates to the protection of data?
Yes☐ No☐

2. Do you have written policies and procedures controlling the introduction and removal of stored data (such as diskettes, tapes, or other storage devices or file attachments to emails) into and out of your facilities by employees or contractors that include the following:

(a) Procedures to control and monitor the ability of individuals to bring hardware, software, or data into or out of your facility?
Yes☐ No ☐

(b) Procedures for maintaining a retrievable, exact copy of all Protected Health Information? Yes☐ No☐

(c) Procedures for the disposition of electronic data, including, among other things, the purging of salvaged, obsolete or redeployed hardware on which data is stored?
Yes☐ No☐

3. Do you have controls to permit physical access to your facilities and systems that include the following:

(a) A process to ensure the retrieval and restoration of data lost as a result of disaster, vandalism, system penetration or failure?
Yes ☐ No ☐

(b) Procedures to enable you to continue operating, and to assure continued access to data, in the event of disaster, vandalism, system penetration or failure?
Yes ☐ No ☐

c) Documented procedures for adding or removing hardware and software from your facilities or systems?
Yes ☐ No ☐

(d) Procedures to secure your premises and equipment from unauthorized physical access, tampering and theft?
Yes ☐ No ☐

(e) Procedures to verify access authorization before granting physical access to your facilities, equipment and systems?
Yes ☐ No ☐

(f) Procedures requiring documentation of all repairs and modifications to the physical components of your security systems?
Yes ☐ No ☐

(g) Procedures that permit user access to systems and data on a need-to-know basis? Yes ☐ No ☐

(h) Procedures to sign in visitors and, where appropriate, provide escorts? Yes ☐ No ☐

(i) Procedures to permit all program testing, revision and modification to authorized personnel?
Yes ☐ No ☐

4. Provide documented instructions regarding allowable workstation use? Yes ☐ No ☐

5. Do you physically isolate or otherwise locate workstations that access sensitive information in areas where they are not likely to be used or viewed by unauthorized persons?
Yes ☐ No ☐

PART 4
TECHNICAL SECURITY SERVICES

1. Do you have in place the following:

(a) A procedure for emergency access to information during a crisis? Yes ☐ No ☐

(b) General access control systems that use either context-based access, role- based access or user-based access controls?
Yes ☐ No ☐

(c) Do you have the capability to encrypt data? Yes ☐ No ☐

(d) Audit controls to record and examine all system use activity? Yes ☐ No ☐

(e) Procedures to validate and corroborate that data in your possession has not been altered or destroyed without authorization?
Yes ☐ No ☐

(0 Do you have systems in place to authenticate that a user is the one it claims to be, including the following:

i. Security procedures that cause an electronic session to terminate after a pre-determined period of inactivity?
Yes☐ No ☐

ii. Required use of a unique user identifier to identify and track individual user activity? Yes☐ No☐

iii. Biometric identification procedures? Yes☐ No☐

iv. Individual passwords in conjunction with user identifiers? Yes☐ No☐

v. Personal identification number (pin) codes in conjunction with user identifiers or passwords?
Yes☐ No ☐

vi. Telephone call-back procedures to authenticate the identity of any remote user? Yes☐ No ☐

2. Tokens or other physical devices to establish user authentication? Yes ☐ No ☐

PART 5
TECHNICAL SECURITY MECHANISMS

1. Do you transmit Personal Health Information over a communications network including, but not permitted, the Internet?
Yes☐ No ☐
2. Do you employ security mechanisms to ensure the validity and integrity of information you electronically transmit and receive our open communications networks?
Yes ☐ No☐

3. Do you employ systems to authenticate that any message received via a communications network matches the message sent?
Yes☐ No ☐
4. Do you employ access controls so that communications transmissions over communications networks cannot be easily intercepted and interpreted by parties other than the intended recipients?
Yes ☐ No ☐

5. Do you encrypt sensitive communications transmissions over communications networks? Yes ☐ No ☐

6. Do your network control systems contain an alarm feature that senses and signals abnormal conditions?
Yes☐ No ☐

7. Do your network control systems provide an audit trail? Yes ☐ No ☐

8. Do your network control systems irrefutably authenticate authorized users and to deny access to unauthorized users?
   Yes ☐ No ☐
9. Do your network control systems generate a network message or other observable response signaling the completion of a requested task as well as operational irregularities?
   Yes ☐ No ☐

VENDOR

by:_____

Name _____

Title_____

Date_____